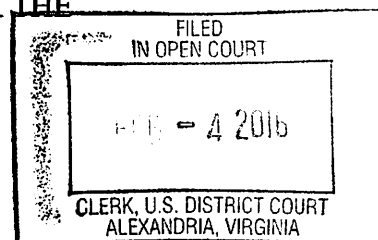


IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

ALEKSEI YURIEVICH BURKOV,
a/k/a "Aleksey Yurevich Burkov,"

Defendant.

CRIMINAL NO.: 1:15-CR-245

Count 1: Conspiracy to Commit Access
Device Fraud (18 U.S.C. § 1029(b)(2))

Count 2: Access Device Fraud
(18 U.S.C. §§ 1029(a)(2) and 2(a))

Count 3: Conspiracy to Commit Wire Fraud
(18 U.S.C. § 1349)

Count 4: Wire Fraud (18 U.S.C. §§ 1343 and 2(a))

Count 5: Conspiracy to Commit Access Device
Fraud, Identity Theft, Computer Intrusion, Wire
Fraud, and Money Laundering (18 U.S.C. § 371)

Forfeiture Notice

Filed Under Seal

FEBRUARY 2016 TERM – AT ALEXANDRIA, VIRGINIA

SUPERSEDING INDICTMENT

THE GRAND JURY CHARGES THAT:

At all times material to this Indictment:

1. Defendant ALEKSEI YURIEVICH BURKOV, a/k/a "Aleksey Yurevich Burkov," is a Russian national who has resided in Tyumen and Saint Petersburg, Russia.
2. The term "carding" refers to various criminal activities associated with stealing financial information and personal identification information belonging to other individuals,

including information associated with credit cards, bank cards, debit cards, or other access devices (collectively, “payment cards”) – and using that information to obtain money, goods, or services without the victims’ authorization or consent. The stolen payment card information often includes, among other things, the card type (e.g., credit or debit), account holder’s name, account number, card verification value or code (“CVV” or “CVC”), and the expiration date of the card. The term “card shop” refers to an online store that sells stolen payment card information. The term “dump” refers to the unauthorized copying of all the information contained in the magnetic strip of an active credit card, such as the card number and expiration date, with the intention of illegally making a fake credit card that can be used by cybercriminals to make purchases.

3. In a typical payment card transaction, after a payment card is swiped through a magnetic stripe reader, the software at the point-of-sale terminal transmits payment card information and transactional information (e.g., price and merchant identification number) electronically to an acquirer. An acquirer is a financial institution that initiates and maintains contractual agreements with merchants for the purpose of accepting and processing payment card transactions. The acquirer electronically routes the transactional and payment card information it receives through the appropriate card network (e.g., Banknet for MasterCard and VisaNet for Visa cards) to the cardholder’s issuing bank to be approved or declined. The credit card issuer receives the transaction information through the card network and checks, among other things, whether the transaction is valid, the cardholder has a sufficient balance, and the account is in good standing. The card issuer then electronically transmits an approval or declination response code through the appropriate card network to the acquirer, which forwards it to the merchant.

4. At all times material to this Indictment, the data center of a particular major U.S. credit card company ("Company-1") for processing payment card transactions was located outside of the Commonwealth of Virginia.

5. At all times material to this Indictment, a major bank that issues credit cards ("Bank-1") had its corporate headquarters in McLean, Virginia, in the Eastern District of Virginia.

6. From at least early 2009 through at least August 2013, BURKOV controlled and operated a card shop known as Cardplanet LLC and Cardplanet.cc ("Cardplanet"), which did business through the website www.Cardplanet.cc (the "Cardplanet Website"). The Cardplanet Website, which contained the user interface for customers who bought stolen payment card data, was hosted on a server located outside the United States. Cardplanet sold payment card data for virtually all major U.S. payment cards, including cards under the Company-1 brand and issued by Bank-1. To date, stolen card data sold on the Cardplanet Website has resulted in estimated fraud losses exceeding \$20,000,000.

COUNT ONE

(Conspiracy to Commit Access Device Fraud)

The Scheme to Defraud

7. From at least early 2009 through at least August 2013, in the Eastern District of Virginia and elsewhere, the defendant,

**ALEKSEI YURIEVICH BURKOV,
a/k/a "Aleksey Yurevich Burkov,"**

did knowingly and with intent to defraud, combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to traffic in and use one and more unauthorized access devices, to wit, payment card account numbers and card verification values, during a one-year period, and by such conduct obtain things of value aggregating \$1,000 and more during that period, to wit, lines of credit associated with numerous payment cards, including, but not limited to, Company-1 cards with account numbers ending in 1149 and 9022, respectively, in violation of Title 18, United States Code, Section 1029(a)(2).

Manner and Means

8. As a part of the fraudulent scheme, in order to promote Cardplanet, BURKOV advertised the Cardplanet Website on underground carding forums to which he belonged. To distinguish Cardplanet from other card shops, BURKOV advertised Cardplanet as the only service that would refund the price of invalid card data. Further, in order to maintain a constant supply of stolen credit and debit card data that would be sold on the Cardplanet Website, BURKOV solicited sales of stolen payment card data by other cyber criminals on carding forums.

9. Through the Cardplanet Website, BURKOV offered for sale data from more than 150,000 compromised payment cards – including cards branded in the names of the largest credit

card companies in the United States – knowing that such stolen data would be used to create counterfeit cards in order to make fraudulent purchases. The price for stolen data from one card varied between \$2.50 and \$60, depending on the card type, country of origin of the card, and the availability of the cardholder's personal identifying information, such as the cardholder's name and address. The compromised cards included at least tens of thousands of cards which had been issued to cardholders in the United States, some of whom were residents of the Eastern District of Virginia. Many of the compromised cards had been issued by Bank-1, which was headquartered in the Eastern District of Virginia.

10. As a further part of the fraudulent scheme, in order to encourage potential customers to buy stolen payment card data from Cardplanet, BURKOV offered a fee-based service, named "checker," on the Cardplanet Website which enabled customers to instantly validate stolen payment card numbers that the customer purchased. BURKOV also promised to replace payment card numbers that were found to be invalid by the checker.

11. Cardplanet accepted payment through digital currency services such as Liberty Reserve and WebMoney, which were favored by cyber criminals because these services generally did not verify the identity of their account holders. Cardplanet also used conventional money transfer systems such as Western Union and MoneyGram, through which transactions could be completed using intermediaries known as "money mules," thereby concealing the true identities of the customers.

12. As a further part of the fraudulent scheme, co-conspirators who purchased stolen payment card data on the Cardplanet Website encoded the data on counterfeit cards embossed with the corresponding payment card company's logo, without the payment card company's knowledge or consent. These co-conspirators then used the counterfeit payment cards to

purchase goods and services from merchants throughout the United States and elsewhere, including merchants located in the Eastern District of Virginia. A portion of the fraudulent purchases were made in person, by presenting the counterfeit payment card to the merchant. Other purchases were made over the Internet, without the fraudulent card being present. To date, the stolen payment card data that BURKOV sold on the Cardplanet Website were used in fraudulent transactions with an estimated aggregate value exceeding \$20,000,000.

Overt Acts

13. It was a further part of the conspiracy that the following acts in furtherance of and to effect the object of the above-described conspiracy were committed in the Eastern District of Virginia and elsewhere:

a. On or about November 13, 2011, BURKOV made a posting on a Russian-language carding forum which advertised the Cardplanet Website as a purveyor of "CVV2 Cards & DUMPS." The posting indicated that prices for "CVV2 Cards" were between \$2.5 and \$10 per card, while the price for "dumps" were between \$12 and \$35.

b. On or about November 17, 2011, BURKOV made another posting on another Russian-language carding forum to promote the Cardplanet Website. That posting indicated that Cardplanet used automated billing through WebMoney and Liberty Reserve, had a good selection of cards and dumps, and based prices on market demand.

c. On or about February 3, 2012, a co-conspirator not named as a defendant herein engaged in a financial transaction at a fast food restaurant in Richmond, Virginia, in the Eastern District of Virginia, using a counterfeit Company-1 small business charge card encoded with stolen card data sold on the Cardplanet Website.

d. On or about March 15, 2013, a co-conspirator not named as a defendant herein engaged in a financial transaction at a convenience store in Fredericksburg, Virginia, in the Eastern District of Virginia, using another counterfeit Company-1 credit card encoded with stolen card data sold on the Cardplanet Website.

e. On or about December 3, 2013, BURKOV sold stolen data for six credit cards to an undercover agent through the Cardplanet Website.

(All in violation of Title 18, United States Code, Section 1029(b)(2))

COUNT TWO

(Access Device Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

14. The factual allegations in Paragraphs 1 through 6 and 8 through 13 are re-alleged and incorporated as if fully set forth here.

15. From at least early 2009 through at least August 2013,

ALEKSEI YURIEVICH BURKOV,

knowingly and with intent to defraud, did traffic in and use one and more unauthorized access devices, to wit, payment card account numbers and card verification values, during a one-year period, to wit, from January 1, 2012, through December 31, 2012, and by such conduct did obtain things of value aggregating \$1,000 and more during that period, to wit, lines of credit associated with numerous payment cards, including, but not limited to, Company-1 cards with account numbers ending in 1149 and 9022, respectively, said trafficking affecting interstate and foreign commerce, in that the trafficking occurred via the Internet, and between computers located inside the Commonwealth of Virginia, and computers located outside of the Commonwealth of Virginia.

(All in violation of Title 18, United States Code, Sections 1029(a)(2) and 2(a))

COUNT THREE

(Conspiracy to Commit Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

16. The factual allegations in Paragraphs 1 through 6 and 8 through 13 are re-alleged and incorporated as if fully set forth here.

17. From at least early 2009 through at least August 2013, in the Eastern District of Virginia and elsewhere, the defendant,

ALEKSEI YURIEVICH BURKOV,

did knowingly combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, the scheme described in Paragraphs 8 through 12, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, payment card-related information was transmitted over the Internet from merchant point-of-sale terminals in the Eastern District of Virginia to computers outside the Commonwealth of Virginia, in violation of Title 18, United States Code, Section 1343.

Overt Acts

18. It was a further part of the conspiracy that the following acts in furtherance of and to effect the object of the above-described wire fraud conspiracy were committed in the Eastern District of Virginia and elsewhere:

a. On or about November 13, 2011, BURKOV made a posting in a Russian-language carding forum which advertised the Cardplanet Website as a purveyor of “CVV2 Cards & DUMPS.” The posting indicated that prices for “CVV2 Cards” were between \$2.5 and \$10 per card, while the price for “dumps” were between \$12 and \$35.

b. On or about November 17, 2011, BURKOV made another posting on another Russian-language carding forum to promote the Cardplanet Website. That posting indicated that Cardplanet used automated billing through WebMoney and Liberty Reserve, had a good selection of cards and dumps, and based prices on market demand.

c. On or about February 3, 2012, a co-conspirator not named as a defendant herein caused a point-of-sale terminal at a fast food restaurant in Richmond, Virginia, in the Eastern District of Virginia, to transmit via the Internet payment card data acquired from the Cardplanet Website to a Company-1 server located outside the Commonwealth of Virginia.

d. On or about March 15, 2013, a co-conspirator not named as a defendant herein caused another point-of-sale terminal at a convenience store in Fredericksburg, Virginia, in the Eastern District of Virginia, to transmit via the Internet payment card data acquired from the Cardplanet Website to a Company-1 server located outside the Commonwealth of Virginia.

e. On or about December 3, 2013, BURKOV sold stolen data for six credit cards to an undercover agent through the Cardplanet Website.

(All in violation of Title 18, United States Code, Section 1349)

COUNT FOUR

(Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

19. The factual allegations in Paragraphs 1 through 6 and 8 through 13 are re-alleged and incorporated as if fully set forth here.

20. From at least early 2009 through at least August 2013, in the Eastern District of Virginia and elsewhere, the defendant,

ALEKSEI YURIEVICH BURKOV,

did knowingly devise and intend to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, the scheme described in Paragraphs 8 to 13, such scheme affecting a financial institution, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, did transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, to wit, payment card-related information was transmitted via the Internet from merchant point-of-sale terminals in the Eastern District of Virginia to computers outside the Commonwealth of Virginia, in violation of Title 18, United States Code, Section 1343.

(All in violation of Title 18, United States Code, Sections 1343 and 2(a))

COUNT FIVE

(Conspiracy to Commit Access Device Fraud, Identity Theft, Computer Intrusion, Wire Fraud,
and Money Laundering)

THE GRAND JURY FURTHER CHARGES THAT:

21. The factual allegations in Paragraphs 1 through 6 and 8 through 13 are re-alleged and incorporated as if fully set forth here.

22. From at least on or about February 21, 2009, through on or about December 13, 2015, in the Eastern District of Virginia and elsewhere, the defendant,

ALEKSEI YURIEVICH BURKOV,

did knowingly combine, conspire, confederate, and agree, with other persons known and unknown to the Grand Jury, to commit a variety of offenses against the United States, including:

- a) To knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, knowing that the means of identification belonged to another actual person, with the intent to commit, and to aid and abet, and in connection with, any unlawful activity that constitutes a violation of Federal law, and that constitutes a felony under any applicable State or local law, where the production, transfer, possession, and use of said means of identification is in and affects interstate and foreign commerce, including the transfer of a document by electronic means, in violation of Title 18, United States Code, Section 1028(a)(7);
- b) To traffic in and use one and more unauthorized access devices during a one-year period, and by such conduct obtain things of value aggregating \$1,000 and more during that period, said use in violation of Title 18, United States Code, Section 1029(a)(2);
- c) To knowingly and with intent to defraud, access a protected computer without authorization and by means of such conduct further the intended fraud and obtain something of value, specifically personal identifying information of others, in violation of Title 18, United States Code, Section 1030(a)(4);
- d) To devise and intend to devise schemes and artifices to defraud, and for obtaining money and property, including the scheme described above in Paragraphs 8 through 12, among others, such schemes affecting financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, including payment card-related information was transmitted

over the Internet from merchant point-of-sale terminals in the Eastern District of Virginia to computers outside the Commonwealth of Virginia, in violation of Title 18, United States Code, Section 1343.

- e) To conduct or attempt to conduct financial transactions which in fact involved the proceeds of specified unlawful activity within the meaning of 18 U.S.C. § 1956(c)(7), knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity, in violation of Title 18 United States Code, Section 1956(a)(1)(B).

Manner and Means of the Conspiracy

23. As part of the conspiracy, BURKOV and his co-conspirators created an online forum (hereafter referred to generically as “the CYBERCRIME FORUM”). The purpose of the CYBERCRIME FORUM was to allow elite cybercriminals to meet in a secure location to plan various cybercrimes, to assist each other in committing cybercrimes, to buy and sell stolen goods and services, including credit card numbers and personal identifying information obtained through illegal computer intrusions, as well as botnets and other malicious software designed for computer hacking, and to assist one another in avoiding detection by law enforcement.

24. It was further part of the conspiracy that BURKOV used the CYBERCRIME FORUM both to advertise and further the unlawful services that he offered, and to locate co-conspirators offering unlawful services that BURKOV desired. These advertisements frequently resulted in BURKOV meeting co-conspirators with whom he would conspire to commit the criminal aims of the conspiracy.

25. It was further part of the conspiracy that BURKOV and his co-conspirators monitored and controlled access to the CYBERCRIME FORUM so as to avoid infiltration from law enforcement. In order to join the CYBERCRIME FORUM, an applicant needed to be “vouched” for by three other members who must state the applicant’s reputation for cybercrime

and history of committing cybercrime. In addition to having trusted members verify an applicant's membership through other cybercrime forums, the vouching members were required to put up an amount of money, usually approximately \$5,000, as insurance in case the applicant failed to make full payment while conducting business on the CYBERCRIME FORUM. Once these preconditions were met, all members of the CYBERCRIME FORUM were able to vote on whether or not to accept the applicant. Once a member was accepted to the CYBERCRIME FORUM, they were required to register with a "moniker," that is, an anonymous online identity. The CYBERCRIME FORUM members monitored the arrests of its members and removed the access of arrested members, i.e. "banned" them from the CYBERCRIME FORUM, in order to prevent law enforcement from using cooperating forum members to access the CYBERCRIME FORUM.

26. It was further part of the conspiracy that BURKOV and his co-conspirators organized the CYBERCRIME FORUM into numerous sections where members can post comments on different topics. These sections, known as forums, were labeled as follows (translated from Russian):

- News
- Stuff Carding-Drops for Stuff, Online Shopping
- Buying and Selling Cards, Visa, MasterCard, and Amex, Looking up SSN/DOB and other card holder information.
- Real Carding, Documents, Real Plastic, Equipment, Dumps (cashing /sales)
- Banking, Drops, account cashing, bank transfers
- Information Security, programing, intrusion, databases, botnets, Trojans, scripts and exploits.

As indicated by their titles, these forums covered such topics as credit card fraud, money laundering, malware¹, hacking, and shipping goods. Members of the CYBERCRIME FORUM

¹ Malware is malicious computer software created to subvert normal operation or take control of a victim computer.

could post “threads” to each forum to discuss a designated topic by posting comments to that threat. Examples of some of the posts on the CYBERCRIME FORUM include members soliciting or requesting to purchase stolen credit card data, members advertising data stolen from hacking, members selling malware to be used in computer intrusions, and members offering to launder the proceeds of cybercrime.

Overt Acts

27. As part of the conspiracy, BURKOV or his co-conspirators committed the following overt acts, among others, in furtherance of and to effect the objects of the conspiracy. These overt acts were committed in the Eastern District of Virginia and elsewhere.

28. On or about February 21, 2009, BURKOV, along with a co-conspirator, launched the CYBERCRIME FORUM.

29. BURKOV, using an online moniker, was active on the CYBERCRIME forum, posting on the site several times per week.

30. On or about November 2011, BURKOV made a posting on the CYBERCRIME FORUM which advertised the Cardplanet Website with the title “Cardplanet.cc CVV2 & Dumps.” The posting stated “We are proud to introduce you to the planet of card.” The purpose and effect of this posting was to drive traffic to the Cardplanet Website so as to aid and facilitate the illegal aims of the website, as described in Counts 1-4 above. As stated in paragraph 13 above, stolen payment card numbers sold on the Cardplanet website were used to commit fraud within the Eastern District of Virginia. Stolen payment card numbers sold and offered for sale on Cardplanet also included cards belonging to residents of the Eastern District Virginia, and cards issued by Bank-1, a major bank that has its corporate headquarters in McLean, Virginia, in the Eastern District of Virginia.

31. On or about November 20, 2015, a co-conspirator and member of the CYBERCRIME FORUM posted an advertisement on the CYBERCRIME FORUM indicating that he wished to sell a database containing the names and dates of birth of over 191 million Americans. This database contains the personal information of American citizens residing in the Eastern District of Virginia.

(All in violation of Title 18, United States Code, Section 371)

NOTICE OF FORFEITURE

1. The factual allegations contained in Counts 1 through 5 of this Indictment are realleged and incorporated by reference for the purpose of alleging forfeiture.

THE GRAND JURY HEREBY FINDS THAT:

2. There is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

3. The defendant is hereby notified, pursuant to Fed.R.Crim.P. 32.2(a), that upon conviction of the offense set forth in Count 1 of this Indictment, the defendant,

ALEKSEI YURIEVICH BURKOV,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(2)(B), and Title 28, United States Code, Section 2461(c), any property, real or personal, involved in such violation, or any property traceable to such property; and pursuant to Title 18, United States Code, Section 1029(c)(1)(C), any personal property used or intended to be used to commit the offense described in Count I of this Indictment. Specifically, the United States seeks forfeiture of:

- a. a sum of money equal to at least \$21,400,000 in United States currency, representing or traceable to the gross receipts obtained as a result of such violation; and
- b. the domain name Cardplanet.cc.

4. Upon conviction of the offense set forth in Count 2 of this Indictment, the defendant,

ALEKSEI YURIEVICH BURKOV,

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), any property, real or personal, constituting, or derived from, proceeds traceable to such violation. Specifically, the United

States seeks a sum of money equal to at least \$21,400,000 in United States currency, representing the amount of proceeds obtained as a result of such violation.

5. If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C); 982(a)(2)(B); 1029(c)(1)(C); and Title 28, United States Code, Section 2461(c), as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Sections 982(b)(1) and 1029(c)(2), to seek forfeiture of all other property of the defendant up to \$21,400,000, as described in paragraph 3 above.

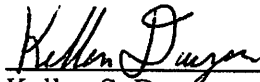
(All pursuant to Title 18, United States Code, Sections 981(a)(1)(C); 982(a)(2)(B); 1029(c)(1)(C), and Title 28, United States Code, Section 2461(c))

A TRUE BILL:

Pursuant to the E-Government Act,
the original of this page has been filed
under seal in the Clerk's Office.

Foreperson of the Grand Jury

DANA J. BOENTE
UNITED STATES ATTORNEY



Kellen S. Dwyer
Assistant United States Attorney

James Silver, Deputy Chief
Harold Chun, Trial Attorney
U.S. Department of Justice
Computer Crime & Intellectual Property Section